IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA,	§	
	§	
Plaintiff,	§	
	§	Criminal No. 3:09-CR-249-D(06)
VS.	§	
	§	
MATTHEW NORMAN SIMPSON,	§	
	§	
Defendant.	§	

MEMORANDUM OPINION
AND ORDER

Defendant Matthew Norman Simpson ("Simpson") moves the court to suppress all evidence seized from his home, office, and business centers, or, alternatively, for an evidentiary hearing. For the reasons that follow, the court denies the motion.[1]

I

Simpson challenges the searches and seizures conducted pursuant to three search warrants issued by United States Magistrate Judge Paul D. Stickney: (1) 3:09-MJ-112, issued on March 30, 2009 for the search of 2323 Bryan Street, Suite 2440, Cage 3, Dallas, Texas 75201 (one of Simpson's business locations); (2) 3:09-MJ-114, issued on March 30, 2009 for the search of 8641 Glenturret, Ovilla, Texas 75154 (Simpson's home); and (3) 3:09-MJ-118, issued on April 1, 2009 for the search of 2323 Bryan Street, Suite 700, Cage 3, Dallas, Texas 75201 (one of Simpson's business locations). Judge Stickney found that there was probable cause to

[1]Pursuant to Fed. R. Crim. P. 12(d), the court sets forth in this memorandum opinion and order its essential findings.

issue warrants for the searches of the premises and the seizure of the specified categories of property. Simpson maintains that all of the evidence seized pursuant to the three search warrants must be suppressed for essentially these reasons: (1) they are general warrants prohibited by the Fourth Amendment; (2) FBI Special Agent Allyn Lynd ("Agent Lynd") included false information in, omitted information from, and relied on stale information in his affidavits; and (3) there is no probable cause to believe that Simpson was connected to the alleged criminal activity.

In the attachments to the affidavits of Agent Lynd that supported each challenged search warrant, Attachment A described the property or premises to be searched and Attachment B described the items to be searched for and seized.[2] The warrants authorized the seizure of 13 categories of items:[3]

> 1. Proceeds, records of proceeds, documents pertaining to, and/or payments related to the conspiracy, computer hardware, and bank records.
>
> 2. Electronic storage devices which consist of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar transmission, reception, collection and storage of data. Electronic storage device includes (but is

[2]The affidavits were executed March 30, 2009 and April 1, 2009 and are nearly identical.

[3]Each warrant authorized the seizure of 12 categories of items designated as Nos. 1-12, and of a category of items, designated as No. 15, consisting of "[a]rticles of personal property which would tend to establish the identity of persons in control of said premises[.]"

not limited to) any wireless/cellular telephone, cordless telephone, pager, fax machine, digital camera, audio recorder, video recorder and any data-processing device e.g. central processing units, memory typewriters, self-contained “laptop”, “notebook”, “mini-notebook”, or “personal data assistant” computers.

3. Any telephonic device which consists of all equipment which can transmit information over any telephone network, assist in said transmission, alter said transmission, disguise such transmission, pay for such transmission, conceal such transmission, and otherwise enhance or degrade such transmission, to include but not limited to telephones, headsets, calling cards, voice alteration devices and software, microphones, speakers, Voice over IP equipment (both hardware and software), ANI altering devices and software, war dialing equipment, etc.

4. Internal and external storage devices e.g. fixed disks (hard drives), memory cards, floppy disk, LS-120, zip drive, jaz drive, Orb drive, CD drive, DVD drive, diskettes, tape drives, optical storage devices, transistor-like binary devices, and other memory storage devices including the storage media used in the devices. Peripheral input/output device such as keyboards, printers, scanners, plotters, video display monitors, and optical readers.

5. Related communication devices e.g. modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices. Any device, mechanism, or parts that can be used to restrict access to electronic storage devices e.g. physical keys and locks bio metric readers, retinal scanners, facial recognition, signature verification, smart card or voice authentication.

6. Computer/Equipment software (digital information) which can be interpreted by electronic storage device equipment, computers and any of its related components to direct the way they work. Software is

stored in electronic, magnetic, optical or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communication programs.

7. Electronic storage device documentation consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use electronic storage device hardware, software, or other related items.

8. Electronic storage device passwords and other data security devices are designed to restrict access to or hide software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

9. A password (a string of alphanumeric characters). A password usually operates as a sort of digital key to “unlock” particular data security devices.

10. Data security hardware, including but not limited to, encryption devices, chips, dongles, biometric readers, retina scanners, facial recognition systems, voice authentication systems, hand writing authentication systems and circuit boards.

11. Data security software or digital code, including but not limited to, programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt; compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

12. Records, notes, address books, calendars, and any other documents that may relate to the violations; magnetic and/or electronic storage media which may contain information relating to the violations; financial records, bank records, correspondence, currency, or other forms of payment that may represent payments related to the violations; property, including manuals, records, media, and work papers, that may relate to trafficking Fraud and Related Activity in Connection with Computers.

> 15. Articles of personal property which would tend to establish the identity of persons in control of said premises, which items of property would consist in part of and include, but not limited to papers, documents and effects which tend to show possession, dominion and control over said premises, including but not limited to keys, canceled mail envelopes, rental agreements and receipts, utility and telephone bills, prescription bottles, vehicle registration, vehicle repairs and gas receipts, whether such items are written, typed or stored electronically.

Federal agents executed the warrants on April 2, 2009, seized items of property from the premises covered by each warrant, and returned the warrants to Judge Stickney on April 13, 2009.

Simpson was charged by indictment on September 1, 2009, by superseding indictment on January 5, 2010, by second superseding indictment on March 24, 2010, and by third superseding indictment on January 26, 2011 with various offenses, including conspiracy to commit wire and mail fraud. He now moves to suppress the seizures and fruits of the seizures and for an evidentiary hearing.

II

Simpson contends that the warrants are general warrants that are prohibited by the Fourth Amendment.

A

Under the Fourth Amendment, "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. "Because indiscriminate searches and seizures conducted under the authority of 'general

warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment, that Amendment requires that the scope of every authorized search be particularly described." *Walter v. United States*, 447 U.S. 649, 657 (1980) (internal quotation marks and citation omitted). "The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another." *Marron v. United States*, 275 U.S. 192, 196 (1927). In other words, the Fourth Amendment proscribes "issuance of general warrants allowing officials to burrow through a person's possessions looking for any evidence of a crime." *United States v. Kimbrough*, 69 F.3d 723, 727 (5th Cir. 1995) (citing *Andresen v. Maryland*, 427 U.S. 463, 480 (1976)). For example, in *United States v. Quinlan*, 149 F.3d 1179, 1998 WL 414295 (5th Cir. July 14, 1998) (per curiam) (unpublished table decision), the panel held a warrant to be general where it authorized seizure of "property that constitutes evidence of the commission of a criminal offense and/or contraband, the fruits of a crime, and/or things criminally possessed." *Id.* at *1.

In reviewing a search pursuant to a warrant, the court engages in a two-step inquiry. *United States v. Payne*, 341 F.3d 393, 399 (5th Cir. 2003). First, the court determines whether the good-faith exception to the exclusionary rule applies. *Id.* (citing *United States v. Pena-Rodriguez*, 110 F.3d 1120, 1129-30 (5th Cir.

1997)). If it does, the court "need not reach the question of probable cause for the warrant unless it presents a 'novel question of law,' resolution of which is 'necessary to guide future action by law enforcement officers and magistrates.'" *Id.* (quoting *Pena-Rodriguez*, 110 F.3d at 1130 n.10). Second, if the good-faith exception does not apply, the court proceeds to a determination of whether "'the magistrate had a substantial basis for concluding that probable cause existed.'" *United States v. Lampton*, 158 F.3d 251, 258 (5th Cir. 1998) (quoting *Pena-Rodriguez*, 110 F.3d at 1129-30).

Simpson primarily argues that the unprecedented volume of seized evidence supports his argument that the warrants are general warrants.[4] But the unprecedented volume of seized evidence may

[4]Although Simpson's motion is far from clear in this respect, he may be arguing that the warrants are so general that no good-faith exception applies to the particularization requirement. "Under the good-faith exception, evidence obtained during the execution of a warrant later determined to be deficient is admissible nonetheless, so long as the executing officers' reliance on the warrant was objectively reasonable and in good faith." *Payne*, 341 F.3d at 399 (citing *United States v. Leon*, 468 U.S. 897, 921-25 (1984)). The good-faith exception cannot apply, however, if "the warrant is so facially deficient in failing to particularize the place to be searched or the things to be seized that the executing officers cannot reasonably presume it to be valid." *Id.* at 399-400 (quoting *United States v. Webster*, 960 F.2d 1301, 1307 n.4 (5th Cir. 1992) (per curiam)). For the reasons that follow, the court concludes that the good-faith exception would apply. The warrant is not so facially deficient in failing to particularize the place to be searched or the things to be seized that the executing officers could not have reasonably presumed it to be valid. But because the court is not relying on the good-faith exception for other purposes, it will address Simpson's challenge without relying on the good-faith exception.

instead reflect the scope of the alleged conspiracy and the criminal activities, which are factors the court can consider in determining whether the warrant meets the particularity requirement. *See, e.g., United States v. Triumph Capital Grp., Inc.*, 211 F.R.D. 31, 57 (D. Conn. 2002); *Andresen*, 427 U.S. at 480-82 n.10 (considering complexity of alleged real estate scheme in holding that list of specific items was not general warrant). In short, the broadness or scope of a warrant does not of itself dictate that the warrant is an unconstitutional general warrant.[5]

> This warrant was broad, to be sure, but it was not "general." The warrant was rather specific about what could be searched and seized. Although the description encompassed virtually all of the business records of the corporation, that does not mean that the warrant lacked particularity; it simply means that it was extremely broad.

United States v. Logan, 250 F.3d 350, 363 (6th Cir. 2001) (citation

---

[5]Simpson apparently relies on *Kremen v. United States*, 353 U.S. 346 (1957), and *Creamer v. Porter*, 754 F.2d 1311 (5th Cir. 1985), to argue that the reasonableness of a search can be judged by the scope of the search and the volume of the seizure. These cases are inapposite. In *Kremen* the court evaluated a warrantless seizure during which the FBI removed the entire contents of the defendants' house. *Kremen*, 353 U.S. at 347. In *Creamer* the executing officers exceeded the scope of the search warrant. *Creamer*, 754 F.2d at 1319. The court evaluated "searches that exceed the permissible scope of a warrant *where items are unambiguously identified* because the Fourth Amendment clearly proscribes such excesses." *Id.* at 1318 (emphasis added).

Simpson does not allege that the searches at issue were conducted without warrants or that the executing officers exceeded the scope of the warrants. Simpson has cited no other authority providing that the scope of the warrants or the volume of seized items is indicative of the particularity of the warrants.

omitted); *see also United States v. Smith*, 424 F.3d 992, 1006 (9th Cir. 2005) ("The warrant's Attachment B describes with sufficient specificity the types of documents and property sought. Potentially problematic is its breadth[.]"). Simpson's argument is therefore misplaced. Particularity does not turn on the volume of what was authorized to be seized or what was seized pursuant to the warrant.

Instead, to determine whether a warrant meets the particularity requirement,[6] the court decides "whether an executing officer reading the description in the warrant would reasonably know what items are to be seized." *Kimbrough*, 69 F.3d at 727. (citation omitted). In some situations, the Fourth Amendment is not violated by the use of generic language. "In circumstances where detailed particularity is impossible, generic language is permissible if it particularizes the *types* of items to be seized." *Id.*[7] "There is no requirement that the government agents know in

---

[6]There is an important difference between a *general* warrant and an *overbroad* warrant. A warrant is *general* where the executing officer would not reasonably know what items are to be seized. A warrant is *overbroad* where probable cause does not support the breadth of the warrant. Simpson appears to argue only that the warrants are general, not that they are overbroad. The court will therefore limit its assessment to whether the warrants are unconstitutionally general.

[7]For example,

> [w]here probable cause exists to believe that an entire business was merely a scheme to defraud, or that all the records of a business are likely to constitute evidence, a warrant

advance the specific items of evidence to be seized or that the items seized do in fact evince a crime, so long as they are within the scope of a properly authorized warrant." *United States v. Cantu*, 774 F.2d 1305, 1308 (5th Cir. 1985) (per curiam). A warrant does not need to specifically identify each document to be seized. *See Triumph Capital*, 211 F.R.D. at 57. The only relevant inquiry is whether, "in light of the nature of the activity under investigation, and the manner of storing the information, [the warrant was] as particular as it could be." *Logan*, 250 F.3d at 363; *see also Triumph Capital,* 211 F.R.D. at 57 ("In determining whether the particularity requirement is satisfied, the court is entitled to place a great deal of weight on whether the warrant is as particular as reasonably could be expected under the circumstances."). And "[t]he complexity of the crimes under investigation is a factor the court may consider in making this determination." *Triumph Capital*, 211 F.R.D. at 57.

"For use involving a scheme to defraud, therefore, a search

> authorizing the seizure of all such records and describing them in generic terms is sufficient to meet the particularity requirement of the fourth amendment.

Williams v. Kunze, 806 F.2d 594, 598 (5th Cir. 1986) (noting that items were described with particularity such that the executing officer had no discretion to decide what could be seized). The court does not suggest that it is finding that defendants' businesses were entirely schemes to defraud. It notes, however, that the more pervasive the alleged fraudulent scheme, the less particular the warrant is required to be.

warrant is sufficiently particular in its description of the items to be seized if it is as specific as the circumstances and nature of the activity under investigation permit." *United States v. Hergert*, 2010 WL 5644670, at *8 (D. Neb. Dec. 30, 2010) (citation omitted), *rec. adopted*, 2011 WL 247328 (D. Neb. Jan. 25, 2011). In *United States v. Humphrey*, 104 F.3d 65 (5th Cir. 1997), the panel held that a warrant authorizing an "all records" search at a residence was valid "where the nature of the fraud was pervasive, there was considerable overlap of the Defendants' business and personal lives, and the warrant limited the search to records pertaining to financial transactions." *United States v. Kim*, 677 F.Supp.2d 930, 942 (S.D. Tex. 2009) (citing *Humphrey*, 104 F.3d at 68). In *United States v. Fiata*, 2006 WL 2544659 (D.S.C. Aug. 30, 2006), the court "[kept] in mind that the search warrant at issue dealt with an investigation of a number of individuals, companies, and separate possible crimes," and found that the warrant met the particularity requirement of the Fourth Amendment because it listed "specific types of records" and went to "some painstaking effort to describe in detail different possible forms of the business records[.]" *Id.* at *8-9. Moreover, "[i]n the investigation of fraud cases, it is difficult——if not impossible——for investigators to discover the precise method and instrumentalities used in perpetuating the fraud before conducting an actual search." *United States v. Cherna,* No. 3:98-CR-072-T, slip op. at 3 (N.D. Tex. July

2, 1998) (Maloney, J.), *aff'd*, 184 F.3d 403 (5th Cir. 1999).

B

The court set forth the relevant background facts and procedural history of this case in its October 19, 2009 memorandum opinion and order and December 28, 2010 order. *See, e.g., United States v. Haney*, 2009 WL 3363821, at *1 (N.D. Tex. Oct. 19, 2009) (Fitzwater, C.J.); *United States v. Faulkner*, No. 3:09-CR-249-D, slip op. at 2-5 (N.D. Tex. Dec. 28, 2010) (Fitzwater, C.J.). The court declared this case complex on October 19, 2009. Nineteen defendants are charged in the third superseding indictment of various crimes, including conspiracy to commit wire fraud and mail fraud. "The government accuses the defendants of being part of a conspiracy that lasted six years (from 2003 to 2009) and involved a loss calculated at approximately [$20] million as of the date of the [third superseding] indictment." *Haney*, 2009 WL 3363821, at *1. "The court has been advised that disclosed digital data in this case exceed 200 terabytes. Ten terabytes of space would hold the printed collection of the Library of Congress[, and] eight terabytes printed would fill 2.72 million banker boxes." *Faulkner*, No. 3:09-CR-249-D, slip op. at 2 n.2. In short, the scope of the alleged conspiracy is wide——it involves nineteen persons, numerous sham companies, and several victim companies——and the alleged criminal activities are primarily electronic in nature.

The warrants in this case authorized seizures of 13 categories

of items. The categories are indeed broad. For example, category two authorizes the seizure of

> [e]lectronic storage devices which consist of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar transmission, reception, collection and storage of data. Electronic storage device includes (but is not limited to) any wireless/cellular telephone, cordless telephone, pager, fax machine, digital camera, audio recorder, video recorder and any data-processing device e.g. central processing units, memory typewriters, self-contained "laptop", "notebook", "mini-notebook", or "personal data assistant" computers.

Although broad, this category lists specific types of items and describes in detail different possible forms of the items in the category. *See, e.g., Fiata*, 2006 WL 2544659, at *8-9. Because of the detailed nature of this category and the examples provided, an executing officer would reasonably know which items were included in the category and which were not. For example, the executing officers seized from Simpson's home his electronic and computer equipment but did not seize his television, musical instruments, or musical equipment. *See* Simpson Aff. 1.

C

Several courts have held that warrants authorizing searches and seizures of categories of items similar to the warrants in this case were sufficiently particular.

In *Cherna* Judge Maloney held that a warrant was sufficiently particular to withstand a Fourth Amendment challenge. *See Cherna*,

No. 3:98-CR-072-T, slip op. at 2-3. The warrant authorized the seizure of records and items "including, but not limited to,"

> 2. Access devices, words, and/or measures including keys, combinations, and passwords, which provide access to locked desk drawers, locked cabinets, locked briefcases, safes, safe deposit boxes, and/or protected computer files, which contain records;
>
> 3. Computers, disks and diskettes, associated hardware and software, computer terminals, computer modems, computer disc drives, central processing units, computer printers, and other associated hardware, manuals, software, and information systems[.]

Brief for Plaintiff-Appellee at 15, *United States v. Cherna*, 184 F.3d 403 (5th Cir. 1999), 1999 WL 33607633. Category 2 in the *Cherna* warrant is similar to categories 8, 9, 10, and 11 in Attachment B. Category 3 in the *Cherna* warrant is similar to categories 1, 2, 4, 5, and 6 in Attachment B.

In *Kimbrough* the panel held that a warrant was sufficiently particular that authorized the seizure of

> [t]apes, cassettes, cartridges, streaming tape, commercial software and manuals, hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media-floppy disks, CD ROMs, tape systems and hard drive, other computer related operational equipment, and other similar materials[.]

Kimbrough, 69 F.3d at 727. The *Kimbrough* warrant lists similar items to those in categories 1, 2, 4, 5, 6, and 7 in Attachment B.

In *Humphrey* the panel concluded that a warrant was sufficiently particular that authorized the seizure of

1. Books, records, receipts, notes, ledgers and other documents relating to financial transactions and relationships with financial institutions.

2. Ledger paper, column paper, check registers, checks, U.S. currency, deposit slips, receipts, bank statements, cashier's checks, association checks, check order forms, new account information forms, wire transfers and receipts, signature cards, correspondence, and all other documents related to banking, banking transactions, and transactions at savings and loan institutions, and in particular all documents relating to the purchasing, cashing, transferring and depositing of cashier's checks.

* * *

4. Computer storage devices containing records, documents, and other information described above in paragraphs 1 thru 3, and related equipment and materials for adequately reviewing the information, including central retrieving and processing units, printers, monitors, floppy discs and instruction manuals which could be used to store information regarding customer files and banking information.

Humphrey, 104 F.3d at 68-69 n.1. Categories 1 and 2 in the *Humphrey* warrant are similar to categories 1 and 12 in Attachment B. Category 4 in the *Humphrey* warrant is similar to categories 2, 4, and 7 in Attachment B.

In *Fiata* the court held that the warrant was sufficiently particular authorizing seizure of

> Any and all business, tax, accounting, financial and investment records, including corporate records, trust records, bank records, investment records, workpapers, correspondence, memoranda, canceled checks, facsimiles, notes, notebooks, telephone and address records, electronic organizers and their contents, pagers and their contents, datebooks, organizers, and tax returns and

> forms . . . .
>
> . . .
>
> (a) computer equipment, including components, and hardware (defined as processing units, hard drives, storage units, interconnecting cables, and peripheral items), computer software, peripherals, storage devices, and access instructions and devices, including floppy diskettes, hard disks, programs, laser disks, CD-ROM, backup disks, tape programs, word processing programs, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernouli drives, electronic notebooks, user manuals, passwords, coded information, keys, and printouts or readouts from any magnetic storage device: and
>
> (b) computer hardware, including computers, central processing units, external and internal drives and external and internal storage equipment or media, terminals or video display units, together with peripheral equipment such as modems, computer or data processing software, or data including, but not limited to, hard disks, floppy disks, magnetic tapes, integral RAM or ROM units, and any other permanent or transient storage device(s); stored electronic mail whether contained on magnetic tape, diskettes, photo-optical devices, or any other medium computer-related documentation, data security devices, manuals for hardware, software, and peripherals, including any and all written or printed material which provides instructions or examples concerning the operation of a computer system, computer software, and or any related devices.

Fiata, 2006 WL 2544659, at *7-8. The introductory category in the *Fiata* warrant is similar to category 12 of Attachment B. Subcategories (a) and (b) are similar to categories 1, 2, 4, 5, 6, 7, 8, and 10 in Attachment B.

In *Smith* the court held that "[t]he warrant's Attachment B describes with sufficient specificity the types of documents and property sought." *Smith*, 424 F.3d at 1006. Attachment B in *Smith* listed eleven categories of items, including:

> 6) All documents relating to the receipt and disbursement of income, by or from any UBO, including credit card receipts and statements, receipts, invoices, statements of accounts at domestic and foreign banks, check registers, cancelled checks, money orders, cashier's checks, wire transfer documents, bank drafts, safety deposit box records, stocks, bonds, and other securities, investment records, loan applications, and other financial statements, promissory notes, telephone toll records and bills, personal calendars, address and telephone books, rolodex indices, records relating to domestic and international travel including tickets, reservations, hotel receipts, travel logs, itineraries, and receipts, Forms 1099 and other tax documents; any other records used to reconstruct income and expenses; records relating to safe deposit box rental.
>
> 7) All documents reflecting current ownership, occupancy, and use of premises including utility bills, receipts, correspondence, monthly statements, photographs, film, and video tapes.
>
> 8) All information and/or data stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer or with the aid of computer-related equipment. This media includes, but is not limited to, floppy diskettes, fixed hard disks, removable hard disk cartridges, laser disks, video cassettes, and any other media which is capable of storing magnetic coding.
>
> 9) All electronic devices which are capable of analyzing, creating, displaying, converting,

> or transmitting electronic or magnetic computer impulses or data. These devices include, but are not limited to, computers, computer components, computer peripherals, word processing equipment, modems, monitors, printers, plotters, encryption circuit boards, optical scanners, external hard drives, and other computer related electronic devices.
>
> 10) All instructions or programs stored in the form of electronic or magnetic media which are capable of being interpreted by a computer or related components. The items to be seized include, but are not limited to, operating systems, application software, utility programs, compilers, interpreters, and any other programs or software used to communicate with computer hardware or peripherals either directly or indirectly via telephone lines, radio, or other means of transmission.
>
> 11) All written or printed material which provides instructions or examples concerning the operation of a computer system, computer software, and/or any related device which is present at the scene.

Id. at 1005-06. Category 6 in the *Smith* warrant is similar to category 1 in Attachment B. Category 7 is similar to category 15 in Attachment B. Categories 8, 9, 10, and 11 are similar to categories 2, 4, 5, 6, 7, and 10 in Attachment B.

In *Logan* the court held that a warrant was broad, but not general, when it authorized the seizure of items in eleven categories, including

> 1) Information and/or data stored in the form of magnetic or electronic coding on computer media or in media capable of being read by a computer or with the aid of computer related equipment. This media includes but is not limited to floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser

disks, video cassettes, and any other media which is capable of storing magnetic coding.

2) Electronic devices which are capable of analyzing, creating, displaying, converting, or transmitting electronic or magnetic computer impulses or data. These devices include but are not limited to computers, computer components, computer peripherals, word processing equipment, modems, monitors, printers, plotters, encryption circuit boards, optical scanners, external hard drives and other computer related electronic devices.

3) Instructions or programs in the form of electronic or magnetic media which are capable of being interpreted by a computer or related components. The items to be seized could include but would not be limited to operating systems, application software, utility programs, compilers, interpreters, and any other programs peripherals either directly or indirectly via telephone lines, radio, or other means of transmission.

4) Printed material which provide [sic] instructions or examples concerning the operation of a computer system, computer software, and/or any related device.

5) Telephone long distance call records and records of wire and electronic interstate communications.

6) Records, files, documents, notes, correspondence, microfiche, or computerized entries concerning the Department of Housing and Urban Development (HUD), Government National Mortgage Association (GNMA), Federal Housing Administration (FHA), manufactured home dealers, borrowers both past and present, payment history and current loan status of borrowers, loan files and accounts of borrowers, loan applications, and copies of submissions to FHA, GNMA, HUD, FHA insurance claims and claims records.

7) Accounts receivable and records thereof.

> 8) Retained copies of documents relating to banking transactions . . . .
>
> 9) Bank correspondence files.
>
> 10) Documents in books of original entry containing entries reflecting any and all transactions, including but not limited to General ledgers, General journals, Subsidiary ledgers, including but not limited to loan loss account ledgers, trial balances, Summary journals including but not limited to cash receipts and cash disbursements, Daily posting records and slips, check request forms, "special handling accounts" and "special handling account" reports.
>
> 11) Internal documents or instructions to employees, representatives or agents concerning GNMA, FHA, borrowers or manufactured homes dealers, personal and informal files, notes, diaries, telephone call logs and telephone records, calendars and working papers of employees and officers of Logan-Laws, Articles of incorporation, or Partnerships.

Logan, 250 F.3d at 362-63. Categories 1 and 2 in *Logan* are similar to categories 2, 4, and 5 in Attachment B. Categories 3 and 5 are similar to categories 6 and 7 in Attachment B. The remaining categories are similar to category 12 in Attachment B.

As set out above, Attachment B to each warrant listed 13 generic, but specific by type, categories of items to be searched for and seized. Given the nature and scope of the alleged conspiracy, it would have been impossible to list each specific item that might be relevant to the alleged crimes. Each warrant,

supported by Agent Lynd's affidavit,[8] listed the applicable categories by types of items with sufficient particularity that the executing agents were limited in their discretion concerning the items that they could lawfully search for and seize. The court therefore holds that the search warrants are not general warrants that are prohibited by the Fourth Amendment. Simpson's motion to suppress is denied in this respect.

III

Simpson also moves to suppress on the ground that false information contained in Agent Lynd's affidavits, information omitted from the affidavits, or stale information in the affidavits led to an error in Judge Stickney's determination of probable cause.

A

Simpson contends that Agent Lynd: (1) falsely identified Simpson as using the alias "Ronald Northern"; (2) omitted knowledge that documents pertaining to Ronald Northern were discovered in a desk not belonging to Simpson; (3) omitted a full description of colocation facilities; and (4) omitted knowledge that he was unable

[8]The affidavit or other incorporated documents may also provide particularization for the items to be seized. *United States v. Kernell*, 2010 WL 1491873, at *18 (E.D. Tenn. Mar. 31, 2010) (citing *United States v. Brown*, 49 F.3d 1162, 1169 (6th Cir. 1995)).

to locate a business identified by an informant.[9] He maintains that the question whether the affidavits deliberately or recklessly misled Judge Stickney requires a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978). Simpson also alleges that Agent Lynd's affidavit relied on stale information and therefore was not supported by probable cause.[10]

B

Under the Fourth Amendment, "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation[.]" U.S. Const. amend. IV. The exclusionary rule precludes the government from relying on illegally-seized evidence. *United States v. Houltin*, 566 F.2d 1027, 1030 (5th Cir. 1978). The purpose of the

[9]It is unclear whether Simpson argues that the misstatements and omissions require a *Franks* hearing, invalidate Judge Stickney's finding of probable cause, or both. Because the court is assuming *arguendo* that Agent Lynd made material misrepresentations and/or omissions, the court will disregard the allegedly material misrepresentations and will consider the allegedly material omissions in determining whether probable cause exists.

[10]Simpson posits that the affidavit relied on a statement of representatives of Waymark Communications ("Waymark") that Suite 2440 and Suite 700 were connected by fiberlink and were essentially the same data center. Simpson argues that because the Waymark representatives visited the Bryan locations in 2007, this information is stale and cannot be used to establish that the two suites were connected. Agent Lynd averred, however, that he visited the Bryan locations and visually confirmed that the equipment located at the Bryan locations substantially met the description provided by the Waymark representatives. Moreover, the court is assuming *arguendo*, *see infra* § III(E) and note 14, that information from 2007 is "stale," even though Simpson has not demonstrated how this undermines Judge Stickney's probable cause determination.

exclusionary rule is to "deter unlawful police conduct." *United States v. Pope*, 467 F.3d 912, 916 (5th Cir. 2006). This purpose will not be served, and thus the rule is inapplicable, where evidence is obtained in "objectively reasonable good-faith reliance upon a search warrant." *Id.* (internal quotation marks omitted).

As noted above, in reviewing a search pursuant to a warrant, the court engages in a two-step inquiry. First, the court determines whether the good-faith exception to the exclusionary rule applies. If it does, the court does not need to reach the question of probable cause unless it presents a novel question of law, the resolution of which is necessary to guide the future actions of law enforcement officers and magistrates. Second, if the good-faith exception does not apply, the court determines whether the magistrate had a substantial basis for concluding that probable cause existed.

"Under the good-faith exception, evidence obtained during the execution of a warrant later determined to be deficient is admissible nonetheless, so long as the executing officers' reliance on the warrant was objectively reasonable and in good faith." *Payne*, 341 F.3d at 399 (citing *United States v. Leon*, 468 U.S. 897, 921-25 (1984)). The good-faith exception cannot apply if "the issuing magistrate/judge was misled by information in an affidavit that the affiant knew was false or would have known except for reckless disregard of the truth[.]" *Id.* at 399 (quoting *United*

States v. Webster, 960 F.2d 1301, 1307 n.4 (5th Cir. 1992) (per curiam)).

In *Franks* the Supreme Court determined that criminal defendants have a limited right under the Fourth and Fourteenth Amendments to challenge the truthfulness of factual statements made in affidavits supporting search warrants, subsequent to the *ex parte* issuance of the warrant. *Franks,* 438 U.S. at 155-56. The *Franks* rule is of "limited scope, both in regard to when exclusion of the seized evidence is mandated, and when a hearing on allegations of misstatements must be accorded." *Id.* at 167. "In *Franks* the Supreme Court held that, under limited circumstances, a defendant is entitled to an evidentiary hearing for the purpose of establishing that a search warrant should be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit." *United States v. Paredes-Moya*, 722 F. Supp. 1402, 1413 (N.D. Tex. 1989) (Fitzwater, J.) (citing *Franks*, 438 U.S. at 155-56), *aff'd in relevant part*, *United States v. Guerra-Marez*, 928 F.2d 665, 671 (5th Cir. 1991) ("The district court properly denied [defendant's] motion to suppress.").

Under *Franks* "[t]here is . . . a presumption of validity with respect to the affidavit supporting the search warrant." *Franks,* 438 U.S. at 171. To be entitled to an evidentiary hearing on suppression, a defendant attacking the validity of an affidavit supporting a search warrant must make a "substantial preliminary

showing" that: (1) the affiant knowingly and intentionally, or with reckless disregard for the truth, made a false statement in the warrant affidavit, and (2) the remaining portion of the affidavit is insufficient to support a finding of probable cause. *Id.* at 155-56, 171; *see also United States v. Dickey,* 102 F.3d 157, 161-62 (5th Cir. 1996); *Paredes-Moya*, 722 F. Supp. at 1413. In other words, "if a search warrant affidavit contains a *material misstatement* made intentionally or with reckless disregard for the truth, the court should excise the offensive language from the affidavit and determine whether the remaining portion establishes probable cause." *United States v. Namer*, 680 F.2d 1088, 1093 (5th Cir. 1982) (emphasis added).[11]

C

The court need not convene an evidentiary hearing under *Franks* because, assuming *arguendo* that the good-faith exception does not apply and that Agent Lynd's affidavits contain misrepresentations and/or omissions that amount to deliberate falsehoods and/or reckless disregard for the truth, the remaining portions of the

[11]Although the court is assuming that the good-faith exception does not apply, Simpson has not made a substantial preliminary showing that Agent Lynd intentionally or recklessly omitted a description of the colocation facilities or that he was unable to locate a business identified by an informant, or that any of the alleged misrepresentations or omissions is material to the determination of probable cause. Simpson has not shown that if a misrepresentation were excised from the affidavit or if an omission were included in the affidavit, the remaining parts of the affidavit would be insufficient to support a finding of probable cause.

affidavits are sufficient to support a finding of probable cause that contraband or evidence of a crime would be found at the three particular places that are the subjects of the search warrants.[12]

The court greatly defers to Judge Stickney's determination of probable cause. *See United States v. May*, 819 F.2d 531, 535 (5th Cir. 1987) (citing *Illinois v. Gates*, 462 U.S. 213, 236 (1983)). In a close case, a warrant is to be presumed valid even though "'it may not be easy to determine when an affidavit demonstrates the existence of probable cause[.]'" *United States v. Phillips*, 727 F.2d 392, 399 (5th Cir. 1984) (quoting *Gates*, 462 U.S. at 236-37). "Probable cause is evaluated utilizing a totality of the circumstances test." *United States v. Campos*, 2010 WL 445932, at *6 (N.D. Tex. Feb. 9) (Fitzwater, C.J.) (citing *Dickey*, 102 F.3d at 162), *appeal docketed*, No. 10-10868 (5th Cir. Aug. 26, 2010). "The

---

[12]For example, in *United States v. Benbrook*, Criminal No. 3:93-CR-180-D (N.D. Tex. July 1, 1993) (Fitzwater, J.), *aff'd*, 40 F.3d 88 (5th Cir. 1994), the court explained:

> This court has noted that to demonstrate a right to a *Franks* hearing, the defendant must make a substantial preliminary showing that a false statement was knowingly and intentionally made by the affiant in the search warrant affidavit. *Franks* exacts strict standards with which defendants must comply before becoming entitled to a hearing. The Fourth Amendment requires that a hearing be convened if the allegedly false statement *is necessary to the finding of probable cause*.

Id., slip op. at 1-2 (emphasis added; citations, internal quotation marks, and brackets omitted).

task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Gates*, 462 U.S. at 238. The reviewing court should look to whether "the magistrate was provided with sufficient reliable information from which he could reliably conclude that the items sought in the warrant were probably at the location sought to be searched." *United States v. Wake*, 948 F.2d 1422, 1428 (5th Cir. 1991) (internal quotation marks and citation omitted).

D

As a preliminary matter, Simpson maintains that no facts alleged in the affidavits connect him to the alleged criminal activity. This argument does not entitle Simpson to relief. On the whole, Simpson's motion attempts to cast doubt on the connection between *Simpson* and the alleged criminal activities; however, the relevant connection for probable cause is between *the places to be searched* and the alleged criminal activities.

This court is to determine whether the magistrate judge had a substantial basis for concluding that "there is a fair probability that contraband or evidence *of a crime* will be found *in a particular place*." *Gates*, 462 U.S. at 238 (emphasis added). Simpson has provided no authority, and the court has found none, that requires that there be a fair probability that contraband or

evidence of a crime will be found *as to a particular suspect or defendant*.[13]

E

Judge Stickney had probable cause to believe that contraband or evidence of a crime would be found at each of the three premises that were the subject of the search warrants. The following facts asserted in the affidavits——facts that Simpson does not challenge in this motion——support this conclusion.[14]

The affidavits generally allege evidence of a conspiracy among several persons to commit wire and mail fraud. Several telecommunications companies advised Agent Lynd that they had been defrauded of at least $6 million by a group of persons operating shell companies that ordered and received services without the intent to pay.

Through Eric Littlejohn ("Littlejohn"), a defendant and alleged coconspirator, Lone Star Power LLC ("Lone Star") ordered services from Verizon to be installed at 2323 Bryan Street, Suite

[13]Simpson also argues that Agent Lynd misidentified him as "Ronald Northern," an alias. But even if this information should be excised from the affidavits, Judge Stickney still had probable cause to issue the search warrants. *See infra* § III(E).

[14]In determining whether the warrants are supported by probable cause, the court (1) does not consider Simpson's identification as Ronald Northern; (2) considers the proper description of colocation facilities; and (3) considers that Agent Lynd could not locate a business identified by an informant. The court also assumes *arguendo* that the information in the affidavits provided by Waymark is stale and disregards this information. *See supra* note 10.

2440, Dallas, Texas 75201. Lone Star did not pay for the services rendered by Verizon, and it owes Verizon $2,204,923.47. The Internet protocol address used by Lone Star when it communicated with Verizon was assigned to NN-Fibernet, and a letter to NN-Fibernet was seen in plain view by Agent Lynd at Simpson's home. Through William Michael Watts ("Watts"), a defendant and alleged coconspirator, Premier Voice Inc. ("Premier Voice") ordered services from Verizon to be installed at 2323 Bryan Street, Dallas, Texas 75201. Premier Voice did not pay for the services rendered by Verizon, and it owes Verizon $2,223,106.49. Premier Voice and Lone Star used the same telephone numbers and address as Incavox, another shell company.

The management of 2323 Bryan Street confirmed that Simpson's computers were located at 2323 Bryan Street, Suite 2440, Cage 3, and that Michael Blaine Faulkner ("Faulkner"), a defendant and alleged coconspirator, had equipment in 2323 Bryan Street, Suites 700 and 2440. The management also told Agent Lynd that Simpson rented a cage on the seventh floor of 2323 Bryan Street under his name, and that the cage was a wire mesh cage shaped like a pie wedge and marked with the number 3.[15]

[15]Simpson appears to argue that there was no probable cause to authorize a search of the specific cages at the Bryan locations. Agent Lynd's affidavits establish, however, that the building manager for the Bryan locations indicated that Simpson's computers were located in Suite 2440, Cage 3, and Suite 700, Cage 3. And Simpson stated that he owned telephone numbers that Judge Stickney could reasonably have believed were associated with criminal

Moreover, Simpson was listed as the registered agent and manager for Core IP Networks LLC ("Core IP"). Core IP provided the original wire transfer and deposit to Verizon for Lone Star's services. Core IP also provided deposit money to Lone Star for services from AT&T. The website of the Texas Comptroller of Public Accounts listed 8641 Glenturret Drive, Ovilla, Texas 75154 as the address for Core IP.

During an interview with Agent Lynd, Simpson stated that (1) he owned Lone Star; (2) his computer servers were located at 2323 Bryan Street, Suites 700 and 2440; (3) he ran all of his businesses from his home; and (4) several of the telephone numbers assigned to Simpson d/b/a Core IP were used by Faulkner. Agent Lynd determined that three of the telephone numbers assigned to Simpson were used by coconspirators in furtherance of the fraud.

Simpson told Agent Lynd that he was assigned the first 1000 block of the telephone number (214) 586-xxxx and that he still administered and controlled the block of numbers. Agent Lynd had determined that three of the telephone numbers had been used to perpetuate the alleged fraud; in particular, Littlejohn used one telephone number for Lone Star Power and Watts used two telephone numbers for Premier Voice. Simpson indicated that he controlled this block of telephone numbers from the data pool located at 2323

---

activities and that the computers were located in the Bryan locations.

Bryan Street, Suites 700 and 2440.

Judge Stickney had a substantial basis for determining that probable cause existed that there was evidence of criminal activity at (1) 2323 Bryan Street, Suite 2440, Cage 3, Dallas, Texas 75201; (2) 8641 Glenturret, Ovilla, Texas 75154; and (3) 2323 Bryan Street, Suite 700, Cage 3, Dallas, Texas 75201. Even without considering the challenged portions of Agent Lynd's affidavits, the remaining parts of the affidavits establish a connection between these three locations and Lone Star, a company that allegedly defrauded Verizon and AT&T. Simpson stated that he ran all of his businesses, including Lone Star, from his home and that his computer servers were located in the Bryan locations.

Accordingly, Simpson is not entitled to a *Franks* hearing or to suppress the searches based on alleged false information contained in Agent Lynd's affidavits, information omitted from the affidavits, or stale information in the affidavits.

* * *

Simpson's December 10, 2010 motion to suppress evidence seized pursuant to search warrants, and all fruits of those seizures, and

for an evidentiary hearing,[16] is denied.

SO ORDERED.

March 2, 2011.

SIDNEY A. FITZWATER
CHIEF JUDGE

[16]In addition to concluding that there is no need to convene a hearing under *Franks*, the court also holds that there is no need to convene a hearing before deciding the other grounds of Simpson's motion. A hearing on a motion to suppress is only required if there are disputed material facts necessary to the decision of the motion. *United States v. Dean*, 100 F.3d 19, 21 (5th Cir. 1996) (per curiam) (citing *United States v. Harrelson*, 705 F.2d 733, 737 (5th Cir. 1983)). Because the court is able to decide Simpson's motion without resolving disputed issues of material fact, an evidentiary hearing is not required.